

**Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, D.C. 20554**

Petition for Expedited Rulemaking to
Establish Technical Requirements and
Standards Pursuant to Section 107(b) of the
Communications Assistance for Law
Enforcement Act

RM-11376

**COMMENTS OF VERIZON ON PETITION FOR EXPEDITED RULEMAKING
TO ESTABLISH TECHNICAL REQUIREMENTS AND STANDARDS PURSUANT TO
SECTION 107(B) OF THE COMMUNICATIONS ASSISTANCE FOR LAW
ENFORCEMENT ACT**

Michael E. Glover, *Of Counsel*

Karen Zacharia
Christopher M. Miller
VERIZON
1515 North Court House Road
Suite 500
Arlington, Virginia 22201
(703) 351-3071

Samir C. Jain
Wilmer Cutler Pickering Hale and Dorr
1875 Pennsylvania Ave., NW
Washington, DC 20006
(202) 663-6000

Attorneys for Verizon

July 25, 2007

**Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, D.C. 20554**

Petition for Expedited Rulemaking to
Establish Technical Requirements and
Standards Pursuant to Section 107(b) of the
Communications Assistance for Law
Enforcement Act

RM-11376

COMMENTS OF VERIZON¹

Verizon has been an industry leader on issues relating to the Communications Assistance for Law Enforcement Act (“CALEA”) and has worked actively with law enforcement and industry standards bodies to help develop and implement CALEA solutions, both for circuit-switched and packet-based services. Verizon remains committed to continuing to do what is necessary to comply with its CALEA obligations. Verizon appreciates that huge increases in the amount and overall size of intercept data over the last several years – increases that could not have been anticipated when CALEA was enacted – pose certain challenges for law enforcement. Verizon, as it always has, remains supportive of law enforcement’s important access to real-time intercepts, and consistent with separate comments filed in this proceeding by Verizon Wireless, Verizon is willing to work with the Department of Justice (“DOJ”) to satisfy statutory objectives. Changes in the timing and manner of delivery of intercept data to law enforcement, however, must be consistent with CALEA and must not impose prohibitive cost limitations on service innovations.

¹ The Verizon companies participating in this filing (“Verizon”) are the regulated, wholly owned subsidiaries of Verizon Communications Inc.

In that connection, to the extent the Commission imposes new requirements for the J-STD-025-B industry standard in response to DOJ's petition,² it should not simply apply those requirements across the board to all other standards. The technical and practical issues that arise in implementing CALEA's capability requirements differ for different services and technologies. Just because a particular technical requirement is cost-effective for CDMA2000 data wireless services (the subject of the J-STD-025-B standard), for example, does not necessarily mean the same requirement would be cost-effective for other services, such as DSL, which uses different equipment and technologies. Thus, in order to modify a particular standard, the Commission must develop a factual record concerning that standard and the services it affects and then determine what modifications, if any, are appropriate in light of that record. This proceeding, which concerns only the J-STD-025-B standard, obviously will not create a record that addresses other CALEA standards. Thus the Commission should make clear that any modifications it adopts here should not automatically be deemed applicable to any standard other than the J-STD-025-B standard.

I. THE TECHNICAL AND PRACTICAL ISSUES RAISED BY THE MODIFICATIONS THAT THE PETITION REQUESTS DIFFER FOR EACH INDUSTRY STANDARD.

A brief review of just some of the changes DOJ requests in its petition as to the J-STD-025-B standard demonstrates the problems and issues that would arise if the Commission were to attempt to impose automatically those same changes for other standards such as the T1.678

² See United States Dep't of Justice Petition for Expedited Rulemaking, filed May 15, 2007 ("Petition").

standard for VoIP and the ATIS-1000013.2007, Lawfully Authorized Electronic Surveillance for Internet Access and Services (“LAES”) standard:³

Reliability – Storage Buffering. DOJ proposes that carriers should be required to guard against the potential loss of packets in intercepted data by storing that data in a buffer and/or co-locating equipment to permit law enforcement to store intercept data. (Petition at 49-50 & n.110.) But, regardless of what the Commission decides as to this issue with respect to the J-STD-025-B standard, there is no basis in this proceeding to impose such requirements in connection with other CALEA industry standards.

A storage or collocation requirement could raise significant technical obstacles and security issues, and may well not be cost-effective (as the statute requires) for various standards such as the LAES standard. The issue of storage buffering has been the subject of much discussion in connection with the development of the LAES standard. In a 2005 submission, for example, law enforcement proposed that carriers store intercept data in a buffer for five days on its own equipment. After discussions in which industry explained the difficulties inherent in such a requirement, law enforcement then proposed a 24-hour storage requirement. In response, the standards development body agreed to write a technical report on the buffering issue. That report is being discussed and both industry and law enforcement have been engaged in extensive and complex discussions regarding the scope and details of any storage or buffering requirement. One of the points at issue, for example, is what happens when the storage capacity of a buffering device is exceeded because of the number of targets subject to interception.

³ In footnote 10 of its petition, DOJ asserts that, to the extent the Commission establishes rules to implement new requirements based on deficiencies it identifies in the J-STD-025-B standard, those rules should apply to other standards. (Petition at 5 n.10.) Presumably, DOJ means only that certain legal conclusions the Commission might reach in this proceeding concerning, for example, the meaning of the term “call-identifying information” might be applicable precedent in assessing the adequacy of other standards.

As this history demonstrates, the imposition of a buffering requirement would raise significant technical issues and might require complex network engineering changes. Depending on factors such as the length of time storage is required, the maximum number of intercepts that carriers must be able to handle, and whether a carrier must maintain separate buffers for different law enforcement agencies (to protect privacy), buffering of intercept data could require massive amounts of storage that would impose significant costs.⁴ Moreover, maintaining this data would raise significant security and chain of custody issues since providers would now have to store and secure significant amounts of intercepted communications. To the extent DOJ suggests that the solution could be implemented through collocation of law enforcement equipment, that raises its own set of security and other practical issues. In addition, it is not clear whether such a solution is workable given Verizon's centralized distribution model for the delivery of intercept information, which would mean all law enforcement agencies would have to co-locate their equipment at the same Verizon location.

There is no reason to assume that the issues raised by a buffering or collocation requirement will be the same for each service and standard given differences in network architectures, equipment, and technologies. Thus, even if the Commission were to conclude that the absence of such a requirement is a deficiency in the J-STD-025-B standard that requires modification of that standard, that determination would not necessarily apply to other standards.

⁴ The amount of storage capacity required could quickly become enormous. In the case of Verizon FiOS data service with 50 Mbps downstream and 5 Mbps upstream, for example, the required storage to implement an intercept order for a single customer over a 24-hour period would be approximately 600 gigabytes, a number that would then have to be multiplied by the number of law enforcement agencies that were requesting an intercept on that customer. The total storage capacity Verizon would have to maintain would depend on, among other factors, the number of simultaneous interceptions required to be performed in Verizon's network.

Instead, in response to a deficiency petition for another standard, the Commission would have to develop a record with respect to that standard.

Location Information. DOJ also argues that the J-STD-025-B standard is deficient because it does not provide adequate information concerning handset location. Again, whether and to what degree handset location should be provided under *other* standards using different technologies presents wholly different questions. Thus, whatever the Commission concludes here with respect to the J-STD-025-B standard cannot be automatically applied to other standards. In particular, as the Commission is aware from its various proceedings concerning E-911, providing location information presents complex issues in the case of VoIP, particularly so-called “nomadic” VoIP services in which carriers rely on customers to enter location information and have little ability to verify its accuracy.⁵ In the case of nomadic VoIP, location information of the type that DOJ apparently desires (e.g., longitude and latitude information) is not “reasonably available” to the carrier, *see* 47 U.S.C. § 1002(a)(2), and would require modifications by both equipment vendors and network providers to develop additional capabilities akin to GPS. Moreover, even where carriers are able to provide location information in the case of E911, that information is provided only when a customer initiates a call to 911. Extending that capability to *all* calls to all numbers would require a very different technical solution. The key point is that what location information is “reasonably available” and whether any additional location requirements would be cost effective will depend on the particular type of service and technology at issue. Accordingly, even if the Commission finds that the J-STD-025-B standard is deficient with respect to location information and imposes additional location

⁵ See, e.g., First Report and Order and Notice of Proposed Rulemaking, *E911 Requirements for IP-Enabled Service Providers*, 20 FCC Rcd 10245, 10259 ¶ 25 (2005) (“[W]e recognize that certain VoIP services pose significant E911 implementation challenges.”).

requirements here, it would require a wholly separate analysis and record to assess that issue as to other standards.

Timing Information. DOJ contends that the J-STD-025-B standard is deficient with respect to timing information. As it concedes, other standards, including T1.678 and LAES, already provide for timing information based on the network timing protocol. In particular, these standards require carriers to time-stamp within 200 milliseconds of acquisition for purposes of accuracy and to deliver within 8 seconds. Although DOJ generally holds out these requirements as a model that the J-STD-025-B standard should match, it also suggests a new requirement – namely, that the time-stamp should include a “time stamp offset” to reflect the local time where the target is located. (Petition at 26 n.63.) Presumably DOJ does not intend this suggestion (in combination with its position that any requirements the Commission imposes here should apply to all other standards) to mean that all standards are deficient to the extent that they do not provide such an offset. There is no basis to conclude that the T1.678 and LAES standards are deficient because they do not provide the time as DOJ desires or that the statute somehow requires that time-stamping be based on any particular time standard. Nor does DOJ provide any evidence that the time-stamping currently provided by the T1.678 and LAES standards are somehow inadequate. Moreover, carriers already have designed their networks and intercept capabilities to provide time-stamping in accordance with the T1.678 and LAES standards, and requiring them to re-engineer their networks to make this change would not be cost-effective as the statute requires.

II. THE APPLICABLE LEGAL STANDARDS CONFIRM THAT MODIFICATIONS TO AN INDUSTRY STANDARD MUST BE MADE ON A STANDARD-SPECIFIC BASIS.

Under the express terms of CALEA, in order to alter an industry standard and promulgate a new rule modifying that standard, the Commission must make two determinations. First, as the

D.C. Circuit explained the last time it reviewed a Commission decision in response to petitions concerning an industry standard under CALEA, before the Commission may modify an industry standard, it has the burden of identifying and explaining how the standard is “deficient” in implementing the requirements of CALEA. *See USTA v. FCC*, 227 F.3d 450, 460-61 (D.C. Cir. 2000) (“Rather than simply delegating power to implement the Act to the Commission, Congress gave the telecommunications industry the first crack at developing standards, authorizing the Commission to alter those standards only if it found them ‘deficient’ Were we to allow the Commission to modify the J-Standard without first identifying its deficiencies, we would weaken the major role Congress obviously expected industry to play in formulating CALEA standards.”).

Second, assuming it identifies such a deficiency, the Commission must find that any alteration it requires meets five statutory criteria. In particular, the proposed new obligation must (1) meet the assistance capability requirements by “cost-effective” methods; (2) protect the privacy and security of communications not authorized to be intercepted; (3) minimize the cost to residential ratepayers; (4) encourage the provision of new technologies and services to the public; and (5) provide a reasonable time and conditions for compliance with and the transition to any new standard. 47 U.S.C. § 1006(b).

Both of the steps in the statutory inquiry are necessarily standard-specific and require a record that addresses the issues as they apply to the standard at issue. To require a modification of one standard based on a record developed with respect to *another* standard would be contrary to law and arbitrary and capricious. Identifying a deficiency in a standard requires that the Commission analyze the specifications of the standard and whether those specifications adequately meet the statutory requirements. Although aspects of this inquiry may be common across all standards (e.g., the legal interpretation of statutory terms such as “call-identifying

information”), other portions clearly will differ across services and technologies – indeed, that is the reason industry and law enforcement have developed different standards for distinct services rather than a single industry standard.

Thus, for example, CALEA requires carriers to provide call-identifying information only to the extent that it is “reasonably available” to them. If, as here, DOJ argues that a standard is deficient because it does not provide certain information that falls within the category of “call-identifying information,” one determination the Commission must make is whether the information in question is “reasonably available” to the carriers in question. The fact that the Commission may find certain information is reasonably available to carriers using CDMA2000 technology, however, is not determinative as to whether that information would be reasonably available to, for example, a DSL broadband access provider or a wireline VoIP provider. Because those services differ in terms of technologies, network architectures, and other factors, the network and other information available to carriers will not necessarily be the same. As a result, the fact that the J-STD-025-B standard may be deficient because it does not provide law enforcement with certain call-identifying information simply does not establish that an industry standard for a different service also is deficient even if it too does not provide that information.

Moreover, it is not clear that the absence of all the capabilities DOJ seeks here constitute “deficiencies” even as to the J-STD-025-B standard. In particular, the lack of a buffering or co-location obligation is not a “deficiency” because CALEA does not require such a capability. The Petition suggests that a buffering or co-location requirement can be grounded in sections 103(a)(1), (a)(2), and (a)(3) of CALEA. (Petition at 42-44, 47-49.) But none of these provisions provide a basis to impose such a requirement. Section 103(a)(1) of CALEA provides that a carrier must be capable of “expeditiously isolating and enabling the government, pursuant to a

court order or other lawful authorization, to intercept . . . all wire and electronic communications carried by the carrier within a service area to or from equipment, facilities, or services of a subscriber of such carrier *concurrently with their transmission to or from the subscriber's equipment, facility, or service, or at such later time as may be acceptable to the government.*" 47 U.S.C. § 1002(a)(1) (emphasis added). In other words, under this provision, a carrier must be able to enable the government to intercept communications "concurrently" with their transmission *or*, if the government agrees and at the *carrier's* option, at some later time. The Petition, however, would have the Commission read this requirement as imposing both an obligation to enable the intercept of communications "concurrently" with their transmission (which the J-STD-025-B standard requires and the Petition does not propose to change) *and* an obligation to store or buffer the intercept data for later use. The statutory language does not impose such a dual obligation on carriers.⁶

Likewise, the statutory requirement in section 103(a)(3) for delivery of intercepted information does not obligate carriers to store intercept data on their premises. To the contrary, that requirement provides that a carrier must be capable of "delivering intercepted communications and call-identifying information to the government, pursuant to a court order or other lawful authorization, in a format such that they may be transmitted by means of *equipment, facilities, or services procured by the government to a location other than the premises of the carrier.*" *Id.* § 1002(a)(3) (emphasis added). Thus, the statute provides that, once a carrier has enabled the government to intercept a communication, it must then deliver the intercept data to a

⁶ Similarly, as to call-identifying information, Section 103(a)(2) requires carriers to enable the government to access call-identifying information "before, during, or *immediately* after the transmission . . . (or *at such later time as may be acceptable to the government.*)" *Id.* § 1002(a)(2) (emphasis added). Again, this section does not require carriers to permit access such information both "immediately after" transmission and at some later time.

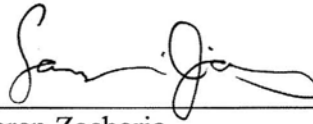
location *other than* the carrier's premises by means of equipment, facilities, or services *procured by the government*.

A requirement to store intercept data on a carrier's equipment on its premises – far from being required by section 103(a)(3) – actually would be contrary to its language, which obligates carriers to deliver the intercept data to a location “*other than*” the carrier's premises by means of equipment, facilities, or services “*procured by the government*.” Similarly, a requirement to store the data on co-located equipment cannot be drawn from a provision that requires delivery “to a location other than the premises of a carrier.” Because CALEA does not impose a requirement for carriers to store intercept data or contemplate co-location of equipment for that purpose, the lack of such an obligation in the J-STD-025-B standard is not a “deficiency,” and the Commission may not alter the standard to impose such a requirement.

CONCLUSION

Whatever modifications the Commission does make to the J-STD-025-B standard, such modifications should not automatically apply across the board to all other industry standards under CALEA. Modifications to an industry standard require standard-specific factual determinations that the Commission could not lawfully make based on the record in this proceeding.

Respectfully submitted,



Michael E. Glover, *Of Counsel*

Karen Zacharia
Christopher M. Miller
VERIZON
1515 North Court House Road
Suite 500
Arlington, Virginia 22201
(703) 351-3071

Samir C. Jain
Wilmer Cutler Pickering Hale and Dorr
1875 Pennsylvania Ave., NW
Washington, DC 20006
(202) 663-6000

Attorneys for Verizon